
Barracuda Spam & Virus Firewall

IT Services has recently implemented a new email security system. The Barracuda Spam & Virus Firewall works to monitor both incoming and outgoing mail, filtering out messages determined to be spam and/or infected with viruses.



Barracuda Spam & Virus Firewall

This guide describes how users can check their quarantined messages, classify messages as spam and not spam, manage whitelisting and blacklisting of email addresses, and modify their user preferences using the Barracuda Spam & Virus Firewall interface.

Quarantined Messages

Messages not positively identified as spam, but are considered suspicious, are quarantined. Users have two options for managing quarantined messages:

1. **Spam Quarantine Summary Report;**
2. **Logging into their Quarantine Inbox.** This is similar to what was in place with Sophos Pure Message.

Option 1 (most users): Spam Quarantine Summary

a) Greeting Message

The first time the Barracuda Spam & Virus Firewall quarantines an email intended for you, the system sends you a greeting message with a subject line of *User Quarantine Account Information*. The greeting message contains the following information:

Welcome to the Barracuda Spam & Virus Firewall. This message contains the information you will need to access your Spam Quarantine and Preferences.

Your account has been set to the following username:

Username: `firstname.lastname@ufv.ca` <your email address>

Access your Spam Quarantine directly using the following link: https://garibaldi.ufv.ca/cgi-mod/index.cgi?user=firstname.lastname@ufv.ca&password=e9bba6b1f0b056a7768f16dfb14513de&et=1348339095&role=_nodomains&locale=en_US

The Barracuda Spam & Virus Firewall will confirm your UFW email address as your username and provide the link to access the quarantine interface. Clicking on the link will take you directly to your Quarantine Inbox.

Most users will want to manage quarantined messages via the Spam Quarantine Summary report which is emailed to you once a day provided:

- Your messages have been quarantined in the last 24 hours and/or
- You have not accessed your Quarantine Inbox directly in the previous 24 hours

b) Spam Quarantine Summary Report

The Barracuda Spam & Virus Firewall sends you a daily summary report so you can view the quarantined messages you did not receive. From the quarantine summary report you can also add messages to your whitelist, delete messages, and have messages delivered to your inbox.

NOTES:

- Each day the quarantine notification service runs for all users.
- If there is no new quarantined mail for your account since the last notification cycle, or if you have logged into your account since then, *no quarantine summary report will be generated and sent to you* for that same 24 hour period.
- Links in the quarantine digest for viewing, delivering, whitelisting or deleting a message from the quarantine inbox **expire in 30 days** from the date the digest is sent out.

The following figure shows an example of a quarantine summary report:

Click to access your quarantine interface to set preferences and classify messages

Select to deliver, whitelist or delete quarantined messages

BARRACUDA NETWORKS Spam Quarantine Summary

Account: **myaccount@somedomain.com**

This is your quarantine summary from the Barracuda Spam & Virus Firewall.

You have **1** messages in your spam quarantine inbox.

- Click on the **Deliver** link to have a message delivered to your mailbox.
- Click on the **Whitelist** link to have a message delivered to your mailbox and whitelist the sender so that his/her messages will no longer be quarantined.
- Click the **Delete** link to have the message deleted from your quarantine.

| Time Received | From | Subject | Actions |
|-------------------|---------------------|----------|--|
| 03/27/09 14:40:32 | janedoe@nowhere.com | sub-quar | Deliver Whitelist Delete |

To view your entire quarantine inbox or manage your preferences, [click here](#).

Spam/Virus Protection By **BARRACUDA NETWORKS**

Option 2: Log In to Your Quarantine Inbox

1. Where to log in

Users can log into their **Quarantine Inbox** directly by pasting the following link into their browser:

<https://garibaldi.ufv.ca>

UNIVERSITY OF THE FRASER VALLEY

Barracuda Spam & Virus Firewall

Login

Please type your email address and password below. If you are the firewall administrator, type your administrative credentials.

Language: English

Username:

Password:

Login

Create New Password

Note: If you forget your password or do not have one, type your email address in the **Username** box. Then click **Create New Password** to have either your existing password or a new one sent to you.

BARRACUDA NETWORKS

NOTES:

- You will not have a Quarantine Inbox until the first time a message sent to you is quarantined.
- The **Create New Password** feature is not applicable so please ignore it.

2. Use the Quarantine Interface

At the end of the Quarantine Summary Report is a link to the quarantine interface where you can set additional preferences and classify messages as spam and not spam.

a) Log into the Quarantine Interface

1. Click the link provided at the bottom of the Quarantine Summary Report (displayed above).
2. The login page appears.
3. Enter your email address as the username and your network password, and click **Login**.

b) Use your Quarantine Inbox

1. After logging into the quarantine interface, select the **QUARANTINE INBOX** tab to view a list of your quarantined messages.
2. When you first start using the quarantine interface, you should view this list on a daily basis and classify as many messages as you can.
3. Clicking on an email displays the message.

c) Add Email Addresses and Domains to Your Whitelist and Blacklist

The **PREFERENCES > Whitelist/Blacklist** page lets you specify email addresses and domains from which you do or do not want to receive emails.

| List Type | Description |
|-----------|--|
| Whitelist | The list of email addresses or domains from which you always wish to receive messages. The only time the Barracuda Spam & Virus Firewall blocks a message from someone on your whitelist is when the message contains a virus or a disallowed attachment file extension. |
| Blacklist | <p>The list of senders from whom you never want to receive messages. The Barracuda Spam & Virus Firewall immediately discards messages from senders on your blacklist. These messages are not tagged or quarantined and cannot be recovered. The sender does not receive a notice that the message was deleted, and neither do you.</p> <p>The only time a blacklisted email address is delivered is if the same email address also appears in your whitelist.</p> |

To whitelist or blacklist senders, follow these steps:

1. Go to the **PREFERENCES > Whitelist/Blacklist** page.
2. A list of your existing whitelisted and blacklisted addresses appears on this page.
3. To delete a whitelist or a blacklist entry, click the trash can icon next to the address.
4. To add an entry, type an email address into the appropriate field and click the Add button.

d) Tips on specifying addresses

When adding addresses to your whitelist and blacklist, note the following tips:

- Entering a **full email address**, such as johndoe@yahoo.com specifies only that user.
- Entering a **domain** such as **barracudanetworks.com**, all users and subdomains are also included (i.e. *support.barracudanetworks.com* and *test.barracudanetworks.com*).
- Mass mailings often come from domains not resembling the company's web site name (i.e. example *historybookclub.com* sends out its mailing from the domain *hbcfyi.com*).
- Examine the From: address of an actual mailing to determine what to enter for an address.